SHEM's Risk Management System (SRMS)

1. Contact Information

A/GIS/IPS Director
Bureau of Administration
Global Information Services
Office of Information Programs and Services

2. System Information

(a) Name of system: SHEM's Risk Management System (SRMS)

(b) Bureau: OBO

(c) System acronym: SRMS

(d) iMatrix Asset ID Number: 116361

(e) Reason for performing PIA:

☒ New system

☐ Significant modification to an existing system

☐ To update existing PIA for a triennial security reauthorization

(f) Explanation of modification (if applicable):

3. General Information

(a) Does the system have a completed and submitted Security Categorization Form (SCF)?
☒Yes
☐No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) What is the security Assessment and Authorization (A&A) status of the system?
The Department of State operates SRMS in accordance with information security requirements and procedures required by federal law and policy to ensure information is appropriately secured. The Department has conducted a risk assessment of the system, identified appropriate security controls to protect against that risk, and implemented the controls. The Department performs monitoring, testing, and evaluation of security controls on a regular basis to ensure that the controls continue to work properly. In accordance with the Federal Information Security Management Act (FISMA) provision for the triennial recertification of this system, SRMS has completed its security assessment and in the process of receiving its Authority to Operate (ATO) once the PIA is approved.

(c) Describe the purpose of the system:

The SHEM's Risk Management System (SRMS) is a web-based application that supports OBO/OPS/SHEM mission requirements by enabling overseas posts to electronically report and manage mishaps, per 15 FAM 954. A "mishap" is any unplanned, unexpected, or undesirable event causing injury, disease or illness, death, material loss or property damage, or incident causing environmental contamination, including improper pesticide application and leaking underground or above-ground storage tanks. The term "mishap" is used instead of "accident" or "occupational illness" and includes motor vehicle accidents.

The system's workflow is designed to ensure that post safety officers (POSHOs) are included in the reporting process and that SHEM conducts a final review before committing the mishap record to the database. The system collects the mishap data using various data entry forms, a drawing applet for diagrams and a file attachment module for photos or documents associated with the mishap. The system contains a number of important report listings and summaries to analyze mishap trends and meet federal injury and illness reporting requirements.

(d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:

- Name, gender, age and date of birth (of the person involved with the mishap);
- Home address and phone numbers (of the person involved with the mishap);
- Post Safety Officer name and government supervisor's e-mail address; and
- Vehicle data

(e) What are the specific legal authorities and/or agreements that allow the information to be collected?

- 29 U.S.C. 688 – Section 19 of the Occupational Safety and Health Act of 1970 (Public Law 91-596);
- Executive Order 12196 – Occupational Safety and Health Programs for Federal Employees;
- 29 CFR 1960 – Basic Program Elements for Federal Employee Occupational Safety and Health Programs;
- 29 CFR Parts 1904 – Recording and Reporting Occupational Injuries and Illness, Occupational Safety and Health Standards; and
- 15 FAM 960 – Safety, Occupational Health, and Environmental Management (SHEM) Program Requirements.

(f) Is the information searchable by a personal identifier (e.g., name or Social Security number)?

☒Yes, provide:

- SORN Name and Number: (1) DOL/GOT-1: Office of Workers' Compensation Programs, Federal Employees' Compensation Act File (2) Security Records. STATE-36.

- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): DOL/GOT-1: April 8, 2002; STATE-36: May 9, 2013.

☐No, explain how the information is retrieved without a personal identifier.

(g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system? ☐Yes ☒No

If yes, please notify the Privacy Division at Privacy@state.gov.

(h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system? ☒Yes ☐No
(If uncertain about this question, please contact the Department's Records Officer at records@state.gov .)

If yes provide:
- Schedule number (e.g., (XX-587-XX-XXX)): A-08-023-03a
- Length of time the information is retained in the system: 5 years or when no longer needed, whichever is later
- Type of information retained in the system:
  Location information including Post Name and location type, time of incident, vehicle information, injured person information, property information, and corrective actions.

4. Characterization of the Information

(a) What entities below are the original sources of the information in the system? Please check all that apply.
☒ Members of the Public
☒ U.S. Government employees/Contractor employees
☐ Other (people who are not U.S. Citizens or LPRs)

(b) If the system contains Social Security Numbers (SSNs), is the collection necessary?
☐Yes ☒No (No SSNs are collected)

- If yes, under what authorization?

(c) How is the information collected?
The information is entered directly into the SRMS system (which is an electronic version of the DS-1663/1664 Mishap Report forms) by OBO personnel or Post personnel (usually the GSO orPOSHO).

(d) Where is the information housed?
☒ Department-owned equipment
☐ FEDRAMP-certified cloud

☐ Other Federal agency equipment or cloud

☐ Other

- If you did not select "Department-owned equipment," please specify.

(e) What process is used to determine if the information is accurate?

SRMS has a validation process which checks that required fields have been entered. Mishap records are routed to a post safety officer and to OBO/OPS/SHEM for verification and coding. The system ensures that data collected is regarding the DOS personnel only. In the event a visitor is injured on DOS property or as a result of a government mishap, the SRMS will collect the non-government person's name, gender and age. If they were a witness, SRMS can collect name, address and phone number.

(f) Is the information current? If so, what steps or procedures are taken to ensure it remains current?

Yes, the SRMS data is collected from the record subjects and maintained in order to meet statutory mishap reporting requirements, to track corrective actions, to provide safety and health performance metrics to DOS management, and to reduce hazards at overseas posts.

(g) Does the system use information from commercial sources? Is the information publicly available?

If an individual did provide the necessary information during the mishap, publicly available information may be used to verify an individual's identity. In order to obtain information on DOS employees, SRMS uses the global address listing (GAL). Additionally, addresses from local listings may be utilized to obtain information regarding local individuals involved in an incident.

(h) Is notice provided to the individual prior to the collection of his or her information?

Yes. Prior to access, the SRMS login screen displays the same Privacy Act statement that is printed on the paper form. This statement reminds the user that they are subject to the privacy policy when utilizing SRMS. Information provided by non-Government employees is voluntary. In some instances their information is initially collected on the hard copy form that contains the Privacy Act statement. A USG employee at post with access to the system would then enter their information into the system.

Additionally, the PIA published on the Department website, as required by the E-Government Act, provides notice to the individuals whose information is collected.

(i) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information? ☒Yes ☒No

- If yes, how do individuals grant consent?

Public individuals have the right to decline to provide information.

- If no, why are individuals not allowed to provide consent?

Federal employees are required to disclose information in order to facilitate an investigation regarding any motor vehicle accident per compliance with 29 CFR

Parts 1904. Those involved are the users completing the forms and creating documentation.

(j) How did privacy concerns influence the determination of what information would be collected by the system?
The information collected by the system is the minimum required PII required for reporting mishaps as indicated on the DS-1663/1664 forms.

5. Use of information

(a) What is/are the intended use(s) for the information?

SRMS data has the following uses:

- To report and file mishap reports from overseas posts to the Bureau of Overseas Building Operations (OBO's) Office of Safety, Health and Environmental Management (SHEM);
- Track the investigation of serious mishaps and review by OBO/OPS/SHEM;
- Track post's corrective actions on all mishaps to prevent reoccurrences;
- Provide quarterly summaries of mishap data to Department management; and
- Analyze trends in accident types, sources and injuries to develop proactive mishap prevention programs and tools (SHEM management can analyze DOS trends while post can only analyze their own).

(b) Is the use of the information relevant to the purpose for which the system was designed or for which it is being designed?
Yes

(c) Does the system analyze the information stored in it? ☐Yes ☒No

If yes:

(1) What types of methods are used to analyze the information?

(2) Does the analysis result in new information?

(3) Will the new information be placed in the individual's record? ☐Yes ☐No

(4) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it? ☐Yes ☐No

6. Sharing of Information

(a) With whom will the information be shared internally and/or externally? Please identify the recipients of the information.
Information may be shared with the Designated Agency Safety and Health Official (DASHO)'s office in MED, upon their request. This typically refers only to serious mishaps in which there is a medical need-to-know (those resulting in hospitalization or a fatality).

(b) What information will be shared?
This sharing with DASHO typically refers only to serious mishaps in which there is a medical need-to-know (those resulting in hospitalization or a fatality). All the information in the mishap report will be shared in that instance.

(c) What is the purpose for sharing the information?
Information is shared so that MED is able to follow up with the DoS employee regarding their medical care and return to work.

(d) The information to be shared is transmitted or disclosed by what methods?
The mishap report is printed out from the SRMS system, scanned, and sent via email to MED when/if needed.

(e) What safeguards are in place for each internal or external sharing arrangement?
Internally: A log is created for any hard copies delivered, where the copy number and recipient's name/org symbol are listed. Hard copies are hand carried to the recipient. If submitted electronically, the information is protected by the safeguards of the Department's internal email system.
Externally: Not applicable, as information is not shared outside the Department.

(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?
The privacy concerns identified are the concerns of the information getting in the wrong hands or in the hands of someone that does not have a need to know. This is addressed, however, by the fact that information in the system is only provided outside of the system in rare occasions. And even in those cases, the only authorized group that the information will be provided to would be MED who is also subject to privacy concerns and responsible for protecting users' PII.

7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?
Individuals are not able to gain access to their information in SRMS. There are no individuals outside of authorized Department users that have access to the system.

(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?

☒Yes ☐No

If yes, explain the procedures.

Individuals can correct their own data until the mishap is "accepted' within the system by amending the reports. After acceptance, amendments to submitted reports can be made through the relevant POSHO or through the SHEM office with administrative control.

If no, explain why not.

(c) By what means are individuals notified of the procedures to correct their information?

Individuals can correct their own data until the mishap is "accepted' within the system by amending the reports. Instructions for how to do this are included in the User's Guide. After acceptance, amendments to submitted reports can be made through the relevant POSHO or through the SHEM office with administrative control.

8. Security Controls

(a) How is the information in the system secured?

The system information is secured based on system role-based security. User access is limited/controlled by their role within the system, so they only have access to information that is necessary for their job responsibilities.

(b) Describe the procedures established to limit access to only those individuals who have an "official" need to access the information in their work capacity.

The system is based on system role-based security. System role is assigned to the user when user requests access to the system. User access is limited/controlled by their role within the system, so they only have access to information that is necessary for their job responsibilities.

(c) What monitoring, recording, and auditing safeguards are in place to prevent the misuse of the information?

Server auditing is configured in accordance with DoS configuration guides and regulations. The application audit function allows the application to generate audit logs containing information that can be quantified by user, event, date and function. The ISSO uses audit monitoring tools including iPost and NetIQ to analyze event audits. Database audit logs are reviewed daily for attempted compromise of the database server. Access to data is restricted to the individuals in the HR department.

(d) Explain the privacy training provided to authorized users of the system.

All users must take PA459 – Protecting Personally Identifiable Information training to safeguard PII. Also, SHEM provides hands-on training, online training, and a user's guide for training purposes. Users must accept the security agreement before they can finish the registration process and gain access to the system.

(e) Are any security controls, such as encryption, strong authentication procedures, or other controls, in place to make the information unusable to unauthorized users? ☒Yes ☐No
If yes, please explain.
The system is Single Sign-On enabled using Department of State's Active Directory, preventing impersonation by any users and preventing any unauthorized users from accessing the system.

(f) How were the security measures above influenced by the type of information collected?
Above security measures are OBO's standard policy of ensuring only authorized users can access OBO Systems and are appropriate for a system that collects PII.

9. Data Access

(a) Who has access to data in the system?
SHEM's users and Post users. In addition to SHEM, other OBO users (Area Management Officers, Program Management Officers, MED, DS), and a Construction Manager (CM) will have access to the system. AMO/PMO access is limited to posts in their portfolio, and DS and CM access is limited to mishaps involved with their personnel. MED HQ has read-only rights within the system.

(b) How is access to data in the system determined?
For Post users, AMOs, PMOs, DS, and CM, it is based on who authors the data and its record. For SHEM's users (and MED HQ), they see all data.

(c) Are procedures, controls or responsibilities regarding access to data in the system documented? ☒Yes ☐No

(d) Will all users have access to all data in the system, or will user access be restricted? Please explain.
Users have limited access to data in the system based on their role that is determined by their position and job responsibilities. Post authors only see mishaps that they create. Other post users only see mishaps that occur at their post. HQ users have access to data related to their job responsibilities. SHEM and MED HQ users see all data.

(e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data?

Individuals accessing the system are assigned roles/privileges based on their "need to know." The level of the individuals' "need to know" is verified by their supervisor before access is granted. Least privilege access is enforced by the application.